ABSTRACT OF THE DISCLOSURE

It is an object of the disclosed technology to provide a tamper resistance device such as a card member having high security. The disclosed technology provides a solution to problems by reduction of the degree of relationship between information processed in the card member such as a chip for an IC card and current consumption for the processing.

As a means for solving the problem, there is provided a method for reducing the degree of relationship between the magnitude of a current consumed by the chip for an IC card and information processed by the chip. In accordance with this method, information is transformed by using data for disturbance of the information prior to processing and, after the processing of the transformed data, the processed transformed information is subjected to inverse transformation using the data for disturbance of the information to result in correct processed information. The method is characterized in that the hamming weight of the data for disturbance of information is all but constant.